UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

| APPLICATION NO. | FILING DATE | FIRST NAMED INVENTOR | ATTORNEY DOCKET NO. | CONFIRMATION NO. |
|---|---|---|---|---|
| 10/784,215 | 02/24/2004 | Sampo Sovio | 4208-4163 (NC28986) | 8410 |

27123 7590 01/31/2008

MORGAN & FINNEGAN, L.L.P.
3 WORLD FINANCIAL CENTER
NEW YORK, NY 10281-2101

| EXAMINER | |
|---|---|
| OKORONKWO, CHINWENDU C | |
| **ART UNIT** | **PAPER NUMBER** |
| 2136 | |

| NOTIFICATION DATE | DELIVERY MODE |
|---|---|
| 01/31/2008 | ELECTRONIC |

**Please find below and/or attached an Office communication concerning this application or proceeding.**

The time period for reply, if any, is set in the attached communication.

Notice of the Office communication was sent electronically on above-indicated "Notification Date" to the following e-mail address(es):

PTOPatentCommunications@Morganfinnegan.com
Shopkins@Morganfinnegan.com
jmedina@Morganfinnegan.com

| Office Action Summary | Application No. | Applicant(s) | |
|---|---|---|---|
| | 10/784,215 | SOVIO ET AL. | |
| | Examiner | Art Unit | |
| | Chinwendu C. Okoronkwo | 2136 | |

*-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --*

**Period for Reply**

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE ____ MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

**Status**

1)☒ Responsive to communication(s) filed on *16 November 2007*.

2a)☐ This action is **FINAL**. 2b)☒ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

**Disposition of Claims**

4)☒ Claim(s) *1-85* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1-85* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

**Application Papers**

9)☐ The specification is objected to by the Examiner.

10)☐ The drawing(s) filed on _____ is/are: a)☐ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

**Priority under 35 U.S.C. § 119**

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

**Attachment(s)**

1) ☒ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☐ Information Disclosure Statement(s) (PTO/SB/08) Paper No(s)/Mail Date _____.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____.
5) ☐ Notice of Informal Patent Application
6) ☐ Other: _____.

## DETAILED ACTION

### *Response to Amendment*

1. In response to communications filed on 11/16/2007, applicant amends several of the claims and adds claim 85. The following claims, claims 1-85 are presented for examination.

1.1 Examiner acknowledges that claim 51 was not addressed in the previous Office Action in err and has thus addressed that claim in the Action.

### *Specification*

2. The amendment filed 11/16/2007 is objected to under 35 U.S.C. 132(a) because it introduces new matter into the disclosure. 35 U.S.C. 132(a) states that no amendment shall introduce new matter into the disclosure of the invention. The added material which is not supported by the original disclosure is as follows: An apparatus comprising: a first network element for storing an application directory having at least one entry, each entry including an application program identifier, attributes, and security parameters; a second network element for determining a priority for each entry in the application directory; a third network element for identifying a selected entry based on the priority; a fourth network element for examining the attributes and the security parameters for the selected entry; and a fifth network element for establishing a security association to support the data communication when the security parameters direct the selected entry to use a secure connection.

Applicant is required to cancel the new matter in the reply to this Office Action.

### *Response to Remarks/Arguments*

3. Applicant's arguments, pages 18-24, with respect to the rejection of claims 1-85 have been fully considered but they are moot in view of the new ground(s) of rejection.

### *Claim Rejections - 35 USC § 103*

4. The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

Claims 1-85 are rejected under 35 U.S.C. 103(a) as being unpatentable over Brownlie et al. (US Patent No. 6,202,157) and further in view of Pandya (US Patent Publication No. 2004/0165588 A1).

Regarding claims 1, 21, 41 and 51, Brownlie et al., discloses a system for controlling data communication in an ad-hoc network that connects a wireless device and a nearby wireless device, comprising: a processor disposed in communication with the memory device, the processor configured to: store an application directory having at least one entry, each entry including an application program identifier, attributes, and security parameters (column 4 lines 31-39

"client application may be a separate program ... each application may have different policy rule data"); determine a priority for each entry in the application directory (column 6 lines 33-38 "policy rule prioritization data ... may be numerical data indicating the level of priority that the policy rule setting data and policy I.D. should obtain in the event that an overriding or underriding policy I.D. is subsequently published"); identify a selected entry based on the priority (column 7 lines 12-15 " once the policy rule setting information has been determined, the client policy engine then determines the rules to enforce and prevents the network node from performing unauthorized actions"); examine the attributes and the security parameters for the selected entry (column 7 lines 2-11 and 41-49 – "security applications identify the application upon first calling of the cryptographic service ... includ[ing] additional information representing the identity of the application for which the policy rule setting applies"); and establish a security association to support the data communication when the security parameters direct the selected entry to use a secure connection (column 7 line 66-column 8 line 24).

Brownlie et al. is silent in disclosing a memory device, however Pandya does such a device (0011 – memory device is equated to - "memory subsystem" and 0087 "remote DMA (RDMA) capabilities").

It would have been obvious for one of ordinary skill in the art, at the time of the invention, to have been motivated to combine the security policy enforcement method and system of Brownlie et al. with the distributed network security system and processor of Pandya because both provide disclosures of network security policy enforcement. Brownlie et al. focuses on the software implementation of such a system, whereas Pandya provides a hardware application to a very similar system. In combination the two provide a complete system in which both approaches are utilized to accomplish the objective of security policy enforcement. Therefore, it would have been obvious to combine the two references as the result and benefit is a system of security policy enforcement in which the software and hardware implementations are utilized.

Regarding the limitations of claims 2, 22, and 42, Brownlie et al. is silent, however Pandya discloses a system of claim 1, wherein the processor is further configured to: receive a connection request from the nearby wireless device (0089 – "described architecture maybe embodied in high performance server ... [like] wireless gateway server"); and send a first application directory to the nearby wireless device (0275 – application directory is equated to "policy rule"); receiving a second application directory from the nearby wireless device (0275); and create the application directory by combining the first application directory and the second application directory (0275 – "develop new rules or security

updates based on the monitored events or other searches or changes in the organizatios policies and create the updates to the policies").

Regarding claims 3, 23, and 43, Brownlie et al., discloses a system of claim 1, wherein the attributes include a device identifier, a role, and control parameters (column 6 lines 33-38 – "policy identification data maybe, for example, a numerical value representing the policy associated with the general category [device attributes]").

[The Examiner's Reasoning: In this example the policy data is related or compared to a password, however it clearly can relate to an application program/software as in column 4 lines 31-39]

Regarding claims 4, 24 and 44, Brownlie et al., discloses a system of claim 3, wherein the control parameters include an application state, and at least one user-defined application setting (column 4 lines 31-39).

Regarding claims 5, 25 and 45, Brownlie et al., discloses a system of claim 1, wherein a bit-string includes the security parameters, a value of the bit-string representing each of the security parameters (column 3 lines 9-24 and 31-43 – bi-string is equated to "digital signature" and security parameters is equated to "policy parameters").

Regarding claims 6, 26 and 46, Brownlie et al., discloses system of claim 1, wherein the security parameters include an information security objective, a cryptography method for attaining the information security objective, and a level of security (column 3 lines 10-24).

Regarding claims 7, 27 and 47, Brownlie et al., discloses a system of claim 6, wherein the information security objective includes maintaining confidentiality, ensuring integrity, authenticating a party, and protecting against replay or reuse (column 3 lines 10-24).

Regarding claims 8, 28 and 48, Brownlie et al., discloses a system of claim 6, wherein the cryptography method includes a signature verification service, and an encryption algorithm (column 4 lines 7-15).

Regarding claims 9, 29 and 49, Brownlie et al., discloses a system of claim 6, wherein the level of security is a minimum required level of security (column 4 lines 18-33).

Regarding claims 10, 20 and 40, Brownlie et al., discloses a system of claim 1, wherein to determine the priority for each entry, the processor is further

configured to: compare the attributes for each entry in said at least one entry (column 7 lines 2-11 and 41-49).

Regarding the limitations for claims 11, 31 and 51, Brownlie et al. is silent, however Pandya discloses a system of claim 1, wherein to establish the security association, the processor is further configured to: query a database for an existing security association between the wireless device and the nearby wireless device that will satisfy the security parameters; reuse the existing security association when the query of the database is successful; and create a new security association when the query of the database is unsuccessful (0274-0276 – "retrieve the corresponding security rules from the rules database and then communicate the rules" and "develop new rules or security policy updates based on the monitored events").

Regarding the limitations for claims 12, 32 and 52, Brownlie et al. is silent, however Pandya discloses a system of claim 11, wherein the processor is further configured to: store the new security association in a connection log, wherein the query of the database includes examination of the connection log (0276 - "log events").

Regarding the limitations for claims 13, 33 and 53, Brownlie et al. is silent, however Pandya discloses a system of claim 11, wherein to reuse the existing

security association, the processor is further configured to: notify the wireless device of the existing security association; notify the nearby wireless device of the existing security association (0089); launch an application program that is referenced by the application program identifier associated with the selected entry when the attributes associated with the selected entry indicate an accommodating state for the launch of the application program (0275); and communicate over the secure connection with a counterpart application program on the nearby wireless device (0089).

Regarding claims 14, 34 and 54, Brownlie et al. idiscloses a system of claim 11, wherein to create the new security association, the processor is further configured to: update the priority of the selected entry to defer the creating of the new security association (column 6 lines 33-44).

Regarding claims 15, 35 and 55, Brownlie et al., discloses a system of claim 11, wherein to create the new security association, the processor is further configured to: establish a privileged side channel to the nearby wireless device; negotiate the new security association over the privileged side channel; and store the new security association (column 7 line 66 – column 8 line 24).

Regarding the limitations for claims 16, 36 and 56, Brownlie et al. is silent, however Pandya discloses a system of claim 15, wherein the privileged side

channel includes a proximity-based communication means, including an infrared data association port, or a direct connection (0089).

Regarding the limitations for claims 17, 37 and 57, Brownlie et al. is silent, however Pandya discloses a system of claim 15, wherein to negotiate the new security association, the processor is further configured to: send authentication data to the nearby wireless device (0012-00113); receive counterpart authentication data from the nearby wireless device (0033); and generate the new security association based on the authentication data and the counterpart authentication data (0275).

Regarding the limitations for claims 18, 38 and 58, Brownlie et al. is silent, however Pandya discloses a system of claim 1, wherein when the security parameters direct the selected entry to use a non-secure connection, the processor is further configured to: notify the wireless device of the non-secure connection;\, notify the nearby wireless device of the non-secure connection, launch an application program that is referenced by the application program identifier associated with the selected entry when the attributes associated with the selected entry indicate an accommodating state for the launch of the application program, and communicate over the non-secure connection with a counterpart application program on the nearby wireless device (0089 and 0275).

Regarding the limitations for claims 19, 39 and 59, Brownlie et al. is silent, however Pandya discloses a system of claim 1, wherein the wireless device initiates the data communication (0089 and 0275).

Regarding for claims 20, 30 and 50, Brownlie et al. discloses a system of claim 1, wherein the wireless device stores the application directory (column 6 lines 33-38).

Regarding claims 60 and 80, Brownlie et al., discloses a system of claim 51, wherein when the security parameters direct the selected entry to use a non-secure connection, further comprising: means for notifying the wireless device of the non-secure connection; means for notifying the nearby wireless device of the non-secure connection, means for launching an application program that is referenced by the application program identifier associated with the selected entry when the attributes associated with the selected entry indicate an accommodating state for the launch of the application program, and means for communicating over the non-secure connection with a counterpart application program on the nearby wireless device (0089 and 0275).

Regarding claims 61, 71 and 81, Brownlie et al., discloses a system for reconnecting to a secure connection in an ad-hoc network that connects a wireless device and a nearby wireless device, the wireless device storing an

application directory having an entry that associates an application program on the wireless device to a counterpart application program on the nearby wireless device, the entry including an application program identifier, attributes, and security parameters, comprising: a memory device; and a processor disposed in communication with the memory device, the processor configured to: store a security association between the wireless device and the nearby wireless device when the nearby wireless device enters the ad-hoc network for a first encounter; store a copy of the security association; remove the security association when the first encounter terminates; and establish a secure connection to the nearby wireless device based on the copy of the security association when the nearby wireless device enters the ad-hoc network for a second encounter (Rejected under the same rationale as claim 1).

Regarding claims 62, 72 and 82, Brownlie et al., discloses a system of claim 61, wherein the storing of the security association is to a short-term storage device (column 2 lines 61-66).

Regarding claims 63, 73 and 83, Brownlie et al., discloses a system of claim 61, wherein the storing of the copy of the security association is to a long-term storage device (column 2 lines 61-66).

Regarding claims 64, 74 and 84, Brownlie et al., discloses a system of claim 61,

wherein to establish the secure connection to the nearby wireless device based on the copy of the security association when the nearby wireless device enters the ad-hoc network for the second encounter, the processor is further configured to: search a connection log to locate the copy of the security association; launch the application program associated with the copy of the security association; configure the secure connection using the security parameters associated with the copy of the security association; and communicate over the secure connection with the counterpart application program (column 2 lines 61-66).

Regarding the limittations for claims 65 and 75, Brownlie et al. is silent, however Pandya discloses a system of claim 64, wherein the processor is further configured to: verify that the copy of the security association will satisfy the security parameters for the second encounter (0274-0276).

Regarding claims 66 and 76, Brownlie et al., discloses a system of claim 64, wherein to search the connection log to locate the copy of the security association, the processor is further configured to: retrieve at least one previous connection from the connection log; and identify one of said at least one previous connection as the copy of the security association (0089 and 0275).

Regarding claims 67 and 77, Brownlie et al., discloses a method for reconnecting to a secure connection in an ad-hoc network that connects a wireless device and

a nearby wireless device, the wireless device storing an application directory having an entry that associates an application program on the wireless device to a counterpart application program on the nearby wireless device, the entry including an application program identifier, attributes, and security parameters, comprising: storing a security association between the wireless device and the nearby wireless device when the nearby wireless device enters the ad-hoc network for a first encounter; storing a copy of the security association; removing the security association when the first encounter terminates; and establishing a secure connection to the nearby wireless device based on the copy of the security association when the nearby wireless device enters the ad-hoc network for a second encounter (Rejected under the same rationale as claim 1).

Regarding claims 68 and 78, Brownlie et al., discloses a method of claim 67, wherein the storing of the security association is to a short-term storage device (column 2 lines 61-66).

Regarding claims 69 and 79, Brownlie et al., discloses a method of claim 67, wherein the storing of the copy of the security association is to a long-term storage device (column 2 lines 61-66).

Regarding claim 85, Brownlie et al., discloses a apparatus, a first network element for storing an application directory having at least one entry, each entry

including an application program identifier, attributes, and security parameters; a second network element for determining a priority for each entry in the application directory; a third network element for identifying a selected entry based on the priority; a fourth network element for examining the attributes and the security parameters for the selected entry; and a fifth network element for establishing a security association to support the data communication when the security parameters direct the selected entry to use a secure connection (column 7 lines 2-11 and 41-49).

***Conclusion***

5. Any inquiry concerning this communication or earlier communications from the examiner should be directed to Chinwendu C. Okoronkwo whose telephone number is (571) 272 2662. The examiner can normally be reached on MWF 2:30 - 6:00, TR 9:00-3:30.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Nasser Moazzami can be reached on (571) 272 4195. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a USPTO Customer Service Representative or access to the automated information system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.

CCO

January 26, 2008

NASSER MOAZZAMI
SUPERVISORY PATENT EXAMINER
TECHNOLOGY CENTER 2100

1/27/08